REMARKS

Claims 1-5, 7-16, 18-26, 28, 29, 31-36, 38-46, 48-52, 54-56, 59-66 are pending for consideration in this application. Claims 1, 2, 5, 7-13, 15, 18-20, 22, 24, 26, 28, 31, 32, 35, 36, 39, 41, 45, 49, 52, 54, 55 and 59-63 have been amended. Claims 6, 17, 27, 30, 37, 47, 53, 57 and 58 have been cancelled without prejudice. Claims 64-66 have been added.

Claim Rejections under 35 USC 112

Claims 5-11, 15-27, 39-41, 47, 53, and 58-62 were rejected under 35 USC 112 second paragraph based on the phrase "substantially simultaneously" in those claims. Without concurring with the Examiner's position, this ground of rejection is not applicable to the claims as now presented and should be withdrawn.

Allowable Subject Matter

It is noted with appreciation that Claim 35 was indicated to be allowable if amended to include all limitations of its parent claim. New claim 65, although not corresponding verbatim to the recitation of claims 28 and 35 is based on the subject matter of those claims and is believed to be allowable together with its dependent claim 66.

Claim 8 was rejected only under 35 USC 112. New claim 64 presents the subject matter of claims 1 and 8 but does not include the subject matter of claim 7 on which claim 8 is directly dependent. Claim 66 is believed to be allowable over the cited art.

It is believed claim 63, similarly to claim 8, also defines allowable subject matter.

Claim Rejections under 35 USC 103

The Examiner's **Response to Arguments** is appreciated even though disagreement remains with at least some of the positions advocated by the Examiner.

Claims 1-7, 9-18, 20-34, and 36-63 have been rejected under 35 USC 103(a) as being allegedly *unpatentable over over* Handbook of Applied Cryptography, Menezes et al., CRC Press 1996, pages 134-168 (Menezes) in view of Quisquater et al., *"Fast Decipherment Algorithm for RSA*

Public Key Cryptosystem", Oct. 1982, Electronic Letters, Vol. 19, No. 21 (Quisquater). The rejections are respectfully traversed.

In rejecting claim 1, the Examiner asserts in Section 5 of the Office Action:

> *". . . Menezes teaches a process of searching for a plurality of prime number values, comprising the steps of: randomly generating a plurality of k random odd numbers each providing a prime number candidate (Sec. 4.1.1, p. 134); and performing a plurality of primality tests on each of the plurality of k randomly generated prime number candidates (Sec. 4.1.1, p. 134), each of the plurality of (k x t) primality tests including an associated exponentiation operation (Sec. 4.2.3 p. 138-140)."*

At Sec. 4.1.1, Menezes discusses generation of large prime numbers using an approach:

> "1. Generate as *candidate* a random odd number *n* of appropriate size.
> 2. Test *n* for primality.
> 3. If *n* is composite, return to the first step."

That is, a candidate (singular) is generated and primality testing is carried out that candidate. Candidates are selected and tested <u>one</u> candidate at a time in a sequential manner – see step 3 above.

The Examiner does concede, properly:

> *"Menezes does not teach a processing system including a processing system including a processing unit and a plurality (k x t) of exponentiation units communicatively coupled to the processing unit, or that the primality tests are carried out by the plurality of exponentiation units in parallel and where the exponentiation operations are carried out substantially simultaneously"."*

The Examiner continues:

> *"However Quisquater et al, teaches such a parallel arrangement of exponentiators (fig. 1, page 2 paragraph 7. Therefore it would have been obvious . . . to incorporate these features into the method of Menezes."*

The Examiner's assertion is respectfully traversed. The Examiner appears to take the position that because Quisquater discloses use of exponentiators operating in parallel in the context of an RSA system, and because Applicant's claimed invention has application in RSA systems, it necessarily follows it would have been obvious to have employed exponentiators operating in parallel in the manner and for the purpose recited in claims 1, 24, 36, 45 and 54. Applicant respectfully disagrees.

In accordance with the current state of the law, when determining the patentability of a claimed invention which combines known elements, the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *Ecolochem Inc. v. Southern California Edison, 56* USPQ2d *1065,* 1073 (Fed. Cir. 2000). In other words, there must be something in the teachings of cited references to suggest to an individual skilled in the art that a claimed invention would have been obvious. *W. L. Gore and* Associates *v. Garlock, Inc.,* 220 USPQ 303 (Fed. Cir. 1983); A concrete suggestion must be present in the cited art for a proper obviousness rejection to be made. *C.R. Bard Inc. v. M3* Systems *Inc., 48* USPQ 2d 1225 (Fed. Cir. 1998).

No such concrete suggestion is present in Quisquater or Menezes. The motivation asserted in the Office Action is:

> *". . . Quisquater teaches such a parallel arrangement of exponentiators (fig. 1, page 2 paragraph 7 –* sic*). Therefore it would have been obvious . . . to incorporate these features into the method of Menezes. It would have been desirable to do so as this would allow for computation tp proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec. 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed."*

This assertion is amplified at page 3 of the Office Action:

> *". . . Section 4.1 of Menezes . . . discusses the advantages of rapid exponentiation parallel processing in the generation of RSA keys, something that would certainly be provided by the system of Quisquater."*

This latter assertion is clearly is erroneous and contradicts the Examiner's own admission (quoted above) that Menezes does **not** disclose primality tests carried out by a plurality of exponentiation units in parallel. Moreover, in Menezes Section 4.1 Introduction, reference to efficient generation of public-key parameters in public key systems such as RSA is not seen to include any discussion providing a "concrete suggestion" for employment of exponentiation units operating in parallel in implementing Menezes procedures which emphasize primality testing of prime number candidates one candidate at a time in a sequential manner, as discussed above. Menezes teaching is seen to be consistent with primality testing procedures and attendant disadvantages discussed in Applicant's specification at page 4, line 22 to page 6, line 20..

The Examiner's position appears to be tantamount to a proposition that because Menezes makes a general observation that "The efficient generation of public-key parameters is a pre-requisite in public-key systems", and Quisquater disclosed operation of exponentiators in parallel (for a purpose that is not seen to be pertinent to Menezes), any employment of parallel exponentiators in Menezes would be preempted as "obvious". Such a sweeping proposition *clearly is untenable, and inconsistent with the required "concrete suggestion" necessary in the* prior art to support a *prima facie* case of obviousness under 35 USC 103, as discussed above.

Considering the Quisquater references as a whole, as required by MPEP 2141.02, Quisquater is seen to disclose how to speed up deciphering a large prime number by breaking it up into smaller length blocks and perform computations on the shorter length blocks which Quisquater observes "may be done in parallel." (Quisquater, p906 (second page) lines 41-61. Thus, the pertinent evaluation of Quisquater is whether the proposed methodology proposed by *Quisquater to implement the computation* $m_1 = c_1^{d1}$ (mod p) and $m_2 = c_1^{d2}$ (mod q)*in parallel* would have suggested employment of that methodology in Menezes system. Applicability of this teaching by Quisquater to Menezes is not apparent from Menezes and no pertinent suggestion or motivation is seen in Quisquater. Menezes discloses (4.51, page 148) selecting a random k-bit odd number n_0 "and then test the *s* numbers $n = n_0, n_0+2, n_0+4, \ldots n_0+2(s-1)$ for primality. " Considering, hypothetically, the Examiner's speculative employment of parallel exponentiators to carry out this particular test (not conceded as being obvious on the basis of Quisquater's teaching)would **not** have resulted in the features of claim 1:

> ". . . *performing a plurality of* **t** *primality tests on each of said plurality of* **k** randomly generated prime number candidates whereby **(k x t)** tests are performed in parallel, each of the plurality of **(k x t)** primality tests including an associated exponentiation operation executed by an associated one of a plurality of **(k x t)** exponentiation units."

Claim 1 requires that a plurality **k** randomly generated prime number candidates **all** be *subjected to a plurality of* **t** *primality tests and that* **all (k x t)** *tests are performed in parallel.* This is beyond any fair implication that might have been derived from Qusisqualter and Menezes. Consequently, claim 1 is believed patentable over Quisquater and Menezes, and for at least similar reasons so are claims 5, 15, 36, 45 and 54.

Claim 24 requires two stages of primaility testing involving initially performing a first primaility test on **s** candidates to yield a remaining number of **r** candidates and performing **(t-1)** primality tests simultaneously on the remaining **r** candidates as recited in claim 24:

> ". . . testing the primality of said sieved candidates by performing a first one of a plurality of **t** primality tests on said sieved number **s** of candidates, each of the plurality **s** of the [[t]] first primality tests including an associated exponentiation operation executed by an associated one of a plurality **s** of the exponentiation units, said exponentiation operations being performed simultaneously by said plurality of **s** exponentiation units units in order to eliminate candidates revealed to be composite numbers thereby yielding a remaining number **r** of candidates; and
> performing a plurality of **t-1** additional ones of said t primality tests on each of said remaining number **r** of candidates, each of the plurality of **(r x (t-1))** first primality tests including an associated exponentiation operation executed by an associated one of a plurality of **(r x (t-1))** of the exponentiation units, said **(r x (t-1))** exponentiation operations being simultaneously performed by said plurality of **(r x (t-1))** exponentiation units in order to eliminate further candidates revealed to be composite numbers."

Such a procedure is not disclosed or suggested by Menezes alone or considered together with Quisquater and the primality testing of the remaining **r** candidates is not obvious over Menezes and Quisquater for at least similar reasons discussed in relation to claim 1. Similar arguments support the patentability of claim 10, 11, 20, 28, 36, 61 and 62.

In reject ting claims 2, 28, 29, 39, 40, 49, 55 and 56, the Examiner relies on Menezes , page 148, Section 4.5.1. The rejections are respectfully traversed. In Section 4.5.1, Menezes only discusses subjecting to a primality test, *s* numbers $n= n_0, n_0+2, n_0+4, \ldots n_0+2(s-1)$ based on a single k-bit odd number n_0. This is not what is claimed in nor does it suggest, by itself or in conjunction with Quisquater, what is claimed in any of these claims.

For example, claim 49 requires:

> "*said processing means is operative to generate a plurality of* **k** *random odd* numbers each providing a prime number candidate, and to determine a plurality of **y** additional odd numbers based on each of said **k** random odd numbers to provide **k x y** additional prime number candidates, thereby providing a total number of at least **k x (y+1)** candidates," (emphasis added)

Menezes thus develops additional candidates based on a single odd number and subjecting these numbers to a primality test. In contrast, claim 49 also requires:

> "said plurality of at least **(k x (y+1) x t)** exponentiation units being operative to perform said plurality of **(k x (y+1) x t)** exponentiation operations in parallel."

Menezes alone or in conjunction with Quisquater simply does not disclose or suggest this parallel, multiple primality testing feature as set forth in claim 49 and claim 49 also is patentable over Menezes considered with Qusisqualter for similar reasons advanced with respect to claim 1.

Claim 2 requires:

> ". . . determining a plurality of **y** additional odd numbers based on each one of the randomly generated numbers $n_{0,0}$, $n_{1,0}$, ... $n_{(k-1),0}$ to provide **(k x y)** additional prime number candidates ($n_{0,1}$, $n_{0,2}$, ... $n_{0,y}$), ($n_{1,1}$, $n_{1,2}$, ... $n_{1,y}$), ...($n_{(k-1),1}$, $n_{(k-1),2}$, ... $n_{(k-1),y}$) thereby yielding a total number of **(k x (y+1))** prime number candidates;"

which is distinguished from Menezes for similar reasons discussed above with respect to claim 49.

Claim 2 additionally requires:

> ". . . performing t primality tests on each of said total number candidates **(k x (y+1))** of prime number candidates, each of the plurality of **(k x (y+1) x t)** primality tests including an associated exponentiation operation executed by an associated one of a plurality of **(k x (y+1) x t)** exponentiation units, said exponentiation operations being performed in parallel by said plurality of **(k x (y+1) x t)** exponentiation units"

This feature renders claim 2 patentable over Menezes and Quisquater for similar reasons to those advanced above with respect to claim 1. Claims 28, 39 and 55 are patentable over Menezes and Quisquater for similar reasons to those discussed with respect to claim 2.

Claims 4, 29, 40 and 56 additionally limit their parent claims by the recitation:

> ". . . determining a plurality of **y** additional odd numbers based on each one of the randomly generated numbers $n_{0,0}$, $n_{1,0}$, ... $n_{(k-1),0}$ includes successively adding two to each of said randomly generated odd numbers $n_{0,0}$, $n_{1,0}$, ... $n_{(k-1),0}$ to provide **(k x y)** additional prime number candidates expressed as ($n_{0,1}$= n_{00}+ 2, $n_{0,2}$=$n_{0,0}$+ 4, ... $n_{0,y}$ = $n_{0,0}$ + (y 2)), ($n_{1,1}$= $n_{1,0}$+ 2, $n_{1,2}$=$n_{1,0}$+ 4, ... $n_{1.y}$ = $n_{1,0}$ + (y

2)), ... ($n_{(k-1),1} = n_{(k-1),0} + 2$, $n_{(k-1),2} = n_{(k-1,0} + 4$, ... $n_{(k-1),y} = n_{(k-1),0} + (y\ 2)$)." (emphasis added)

Again, as discussed with respect to claim 49, this features is not disclosed or suggested by Menezes who emphasizes performing one primality test at a time. Claims 4, 29, 40 and 56 are thus patentable over Menezes and Quisquater for this reason as well as the reasons advanced with respect to their parent claims.

The rejections of the remaining pending claims 3, 7-13, 16, 18-23, 25, 26, 31-35, 38-44, 46, 48, 50-52, 58-60 and 63 are traversed and those claims are believed to be allowable together with their parent claims.

CONCLUSION.

It is believed this amendment and response have addressed all grounds of rejection contained in the Office Action and has placed all pending claims in condition for allowance. Accordingly, favorable consideration and early allowance of the applications are respectfully solicited. If there are any remaining issues that could be resolved by discussion, a telephone call to the undersigned attorney at (425) 402-4638 would be appreciated.

Date: November 30, 2005
Hewlett-Packard Company
Intellectual Property Administration
PO Box 272400
Fort Collins, CO 80527-2400

Respectfully submitted,

N. Rhys Merrett

N. Rhys Merrett
Attorney for Applicant
Reg. No. 27,250